



---

# **UNRAVELING 'SOX'**

## **An Overview of Internal Controls (Sec. 302)**

---

Copyright MIEL e-Security Pvt Ltd  
Author: Rion Dutta

### **WHITEPAPER**

## Contents

---

1] Why SOX?	Pg - 2
2] Internal Controls & Sec. 302	Pg - 3
3] Going by the rulebook	Pg - 4
4] But how do we do that	Pg - 5
5] Conclusion	Pg - 6

# UNRAVELING 'SOX'

## An Overview of Internal Controls (Sec. 302)

---

Copyright MIEL e-Security Pvt Ltd

Author: Rion Dutta

### December 2002:

*A major brokerage house on Wall Street, Company A's system crashes 'inexplicably' when a few employees try to access the corporate network after the weekend. The usual procedures are followed – call help desk, log a trouble ticket, wait for a 'fix'...*

*Except, in this instance, Company A didn't realize the extent of damage that a seemingly routine system outage could cause.*

*Later, investigations revealed that a disgruntled ex-employee had corrupted the systems, triggered to crash, when hundreds of users at Company A, accessed the trading platform interface. The employee in question, gambled on the fact that Company A's stock would crash, along with its systems, and benefited from the numerous put options that he had placed on the stock.*

*Eventually, Company A spent 3 Million US\$ to assess and repair the damage, not to speak of untold loss of goodwill and public faith when the network channels picked up the news.*

### Why SOX?

The Sarbanes-Oxley Act of 2002, or SOX, was passed by Congress, to restore confidence in financial markets, which had been battered by a series of high profile cases of deception and fraud, resulting in the loss of

billions of dollars in shareholder wealth and value. The creators of the law wanted to create legislation that would clearly identify responsibility for compliance and also hold them accountable for any failures. While the deadline for SOX compliance has been determined on the basis of market capitalization, all companies that are traded in the US financial markets have to comply within a timeframe, with heavy monetary penalties and even prison terms for knowingly violating the Act.

Although SOX, as it is commonly referred to, scrutinizes the financial reporting systems of companies, the truth is that financial systems are tightly integrated with the IT infrastructure and therefore, SOX compliance needs to take into account any systems which are interoperable with the core financial accounting function. Central to a SOX implementation are internal controls. While SOX holds certifying officers responsible for establishing internal controls, which will attest to the integrity and veracity of accounting and reporting systems, it does not specify in detail what is required to achieve compliance.

### **Internal Controls & Sec. 302:**

Section 302 SOX holds special significance, as it specifically relates to establishing and maintaining internal controls.

The term internal control, as defined in the final SEC rules manual for implementing SOX, is defined as '...a process designed by or under the supervision of the registrant's principal executive and principal financial officers...to provide reasonable assurance regarding financial reporting and the preparation of financial statements for external purposes in accordance with GAAP...and includes those policies and procedures that:

1. Pertain to the maintenance of records that accurately maintain transactions

2. Provide reasonable assurance that transactions are recorded in compliance with GAAP, and that the said transactions are being made with the requisite authorizations of management and directors of the registrant.
3. Provide reasonable assurance regarding prevention or timely detection of unauthorized transactions that could have a material effect on the registrant's financial statements.

In a nutshell, SOX ensures that top management gets accurate information from subordinates and reports it to the SEC. The goals are to ensure that financial reports that are made to shareholders are truthful and accurate, and to prevent executive officers from blaming faulty reporting systems or breakdowns in procedures for lapses.

### Going by the rulebook:

So what does compliance entail? Most companies have internal controls in place – but SOX requires that those controls be examined and, if necessary, strengthened.

The first section in Section 302 of SOX refers to maintenance of records. Companies must adopt policies and procedures that ensure that electronic records of transactions and asset disposals must be retained and maintained.

For example, for a company that does most of its planning and budgeting in the form of individual spreadsheets, this represents a mammoth task of combining all the information into a financial reporting database. It is only through the use of technology, and adequate policies and safeguards that companies can expect to 'clean up' their record keeping procedures.

The second section is no easier – its purpose is to discourage and penalize 'off the book' transactions and manipulations of revenue, the

kind which have resulted in many violations of the SEC's corporate governance rules and have resulted in many companies having to restate their revenues for several years. Compliance requires changes in internal processes and also an information security framework that can detect control violations in the processes where technology is used.

The third section clearly refers to information security policies and procedures, as part of a company's compliance initiatives. Since information assets, including data volumes, are treated as corporate assets, '...prevention or timely detection of unauthorized acquisition, use or disposition of...assets', any company not wanting to run foul of SOX needs to implement necessary information security controls. Customer databases, product development information and classified trade information are examples of assets, the loss of which would materially impact the financial position of the company, and therefore must be protected.

### But how do we do that?

The Sarbanes-Oxley Act, though has not specified any standards that should be referred to, while preparing and evaluating internal controls. Instead, regulated parties need to refer to other established standards for guidelines. Two standards are frequently cited – COBIT (Control Objectives for Information and Related Technology) and COSO (Committee of the Sponsoring Organizations). While COSO is an accounting standard, which focuses on reporting and operations controls on the accounting system, it does not focus on information security controls other than state their importance. So, to identify and evaluate IT controls, organizations commonly turn to COBIT, as it focuses on IT governance using a framework of control objectives to ensure that the company's IT infrastructure sustains its objectives and supports its strategies.

The COBIT standard is divided into 4 major domains (planning and organization, acquisition and implementation, delivery and support, monitoring and evaluation), and 34 processes, and addresses five major focus areas – strategic alignment, delivery, risk management, resource management and performance management.

This paper does not attempt to provide a detailed implementation plan – but to narrow down the scope and requirements for 'Implementation of Internal Controls'. While COBIT addresses the requirement to setup internal controls, many parts of COBIT also relate to measures that meet COSO components – a SOX implementation that relies on COBIT is the best approach to defining and maintaining internal controls.

It is important to understand that when designing internal controls, it is equally necessary (and now mandatory under the SOX regime) to ensure that these controls actually work. This means periodic evaluation by the company's executive management, and, as specified by the Act, within 90 days of the annual SOX compliance statement that companies must now report.

SOX specifies that the chief executive officer and chief financial officer must certify the internal controls and also state their conclusions about the effectiveness of these controls as part of a SOX compliance statement. Again, this means that information security processes must be tested at least quarterly, and lapses will automatically show up in the disclosure statement with sanctions being imposed on the executive officers and the company.

## Conclusion:

The actions of the SEC till date, whilst investigating companies for violations of its corporate rules, indicate that the regulatory body is getting tougher on offences and violations. From 91 active investigations in 1997, to 149 in 2002, the SEC has made its intentions clear – it is

going to go after errant companies and their office bearers with a renewed vigor. SOX is more than a toothless mandate – it identifies the guilty and enables prosecutors to go after them with plenty of ammunition.

But there are obvious benefits that can be attributed to a company's compliance with SOX. While commenting on the improved corporate governance environment that exists today, the Wall Street Journal commented... 'judging by public opinion, the law is a hit. A Harris poll found 59% of investors believe that the Sarbanes Oxley Act will improve the value of their investments, and 57% unlikely to invest in a company that didn't comply with the law. Supporters say that investors are regaining their faith in markets, and view the Sarbanes Oxley Act as a key factor'

As GE's General Counsel, put it, without mincing his words:

*'Sarbanes-Oxley has nothing to do with culture. You either have it or you don't. If you don't have it, you better get it.'*



## Reach us at:

---

MIEL e-Security Pvt. Ltd.: C – 611 / 612, Floral Deck Plaza  
MIDC Central Road, Andheri (East), Mumbai 400 093. INDIA  
Tel # General: +91 22 28215050 | Tel # Training: +91 22 39560003 / 04 | Fax#: +91 22 28215838  
Email – General: [feelsecure@mielesecurity.com](mailto:feelsecure@mielesecurity.com) | Email – Training: [isti@mielesecurity.com](mailto:isti@mielesecurity.com)  
Website: [www.mielesecurity.com](http://www.mielesecurity.com)

---